ELSEVIER

Theoretical Computer Science 230 (2000) 235–245

Theoretical Computer Science

www.elsevier.com/locate/tcs

The variety of Kleene algebras with conversion is not finitely based

S. Crvenković[a], I. Dolinka[a], Z. Ésik[b,*,1]

[a] *Institute of Mathematics, University of Novi Sad, Trg Dositeja Obradovića 4, 21000 Novi Sad, Yugoslavia*

[b] *Department of Computer Science, Institute of Informatics, A. József University, Árpád tér 2, 6720 Szeged, Hungary*

Received March 1998; revised November 1998

Communicated by M. Ito

Abstract

Given an arbitrary set A, one obtains the full Kleene algebra of binary relations over A by considering the operations of union, composition, reflexive-transitive closure, conversion, and the empty set and the identity relation as constants. Such algebras generate the variety of Kleene algebras (with conversion). As a result of a general analysis of identities satisfied by varieties having an involution operation, we prove that the variety of Kleene algebras with conversion has no finite equational axiomatization. In our argument we make use of the fact that the variety of Kleene algebras without conversion is not finitely based and that, relatively to this variety, the variety of Kleene algebras with conversion is finitely axiomatized.

1. Introduction

For any set A, we can consider a number of operations that are defined for binary relations over A. Such operations are, for example, union $+$, composition $\cdot$, reflexive-transitive closure * and conversion of relations denoted $^\vee$. Thus, one obtains the *full Kleene algebra of relations on A* [13]:

$$\mathbf{Rel}^\vee(A) = (\mathscr{P}(A \times A), +, \cdot, ^*, ^\vee, 0, 1),$$

where 0 is the empty relation and 1 denotes the identity relation. If we omit the conversion operation $^\vee$, we obtain the algebra $\mathbf{Rel}(A)$.

* Corresponding author.

E-mail address: esik@inf.u-szeged.hu (Z. Ésik)

[1] Partially supported by Grant T22435 from the Hungarian National Foundation for Scientific Research, Grant 247/1999 from the Higher Education Research and Development Fund of Hungary and by Grant no. 351 of the US-Hungarian Joint Fund.

0304-3975/00/$ - see front matter
PII: S0304-3975(99)00079-1

Now we define $\mathscr{KA}^{\vee}$ to be the variety generated by all algebras $\mathbf{Rel}^{\vee}(A)$, called the variety of *Kleene algebras*. Similarly, the variety $\mathscr{KA}$ of *conversion-free Kleene algebras* is the one determined by all algebras $\mathbf{Rel}(A)$.

The aim of this note is to present proofs of the assertion that $\mathscr{KA}^{\vee}$ has no finite base for its equations, which intuitively means that the conversion does not "mix up" the rational part of the equational theory of $\mathscr{KA}^{\vee}$, as $\mathscr{KA}$ is well known to be nonfinitely based, see [4, 5, 16, 17].

Actually, we are going to give two separate proofs of this assertion, both using the fact, proved in [8], that $\mathscr{KA}^{\vee}$ has a finite axiomatization over $\mathscr{KA}$. Our first argument is rather syntactic but quite general and has some other applications. The second argument is based on Krob's methods, see [14], which employ some of Conway's ingenious constructions [4]. These constructions will be appropriately modified, and that modification, together with the axiomatization of [8] will yield the desired proof.

2. A general fact on involution algebras

For basic notions of universal algebra we refer to [12].

Suppose that Σ is a finite signature consisting of a set of n-ary operation symbols Σ_n for each $n \geqslant 0$. The signature $\Sigma^{\vee}$ is obtained from Σ by adding the unary symbol $^{\vee}$ to Σ_1. Thus $\Sigma_1^{\vee} = \Sigma_1 \cup \{^{\vee}\}$ and $\Sigma_n^{\vee} = \Sigma_n$, for all $n \neq 1$. The *involution equations* (with respect to Σ) are the equations

$$(\sigma(x_1, \ldots, x_n))^{\vee} = \sigma(x_n^{\vee}, \ldots, x_1^{\vee}), \tag{1}$$

$$(x^{\vee})^{\vee} = x, \tag{2}$$

where σ is a symbol in Σ_n, $n \geqslant 0$. Note that when $n = 0$ Eq. (1) becomes $\sigma^{\vee} = \sigma$. Any $\Sigma^{\vee}$-algebra satisfying (1) and (2) is called an *involution Σ-algebra*.

Suppose that $\mathscr{V}$ is a nontrivial variety of Σ-algebras. We let $\widehat{\mathscr{V}}$ denote the variety of involution $\Sigma^{\vee}$-algebras satisfying all equations true in $\mathscr{V}$. Thus, the Σ-reduct of any algebra in $\widehat{\mathscr{V}}$ is in $\mathscr{V}$. In this section we will prove Corollary 2.4 which gives conditions that a subvariety $\mathscr{W}$ of $\widehat{\mathscr{V}}$ be finitely based. Before stating this result, we need some definitions and notation.

We let X denote a countably infinite set of variables $x_1, x_2, \ldots$ used to construct $\Sigma^{\vee}$-terms, or terms, for short. A term which contains no occurrence of the symbol $^{\vee}$ is a Σ-term. Suppose that t is a term. The positive normal form t^+ and negative normal form t^- of t are defined as follows.

1. If $t = x$, for some $x \in X$, then $t^+ = x$ and $t^- = x^{\vee}$.
2. If $t = \sigma(t_1, \ldots, t_n)$, where $\sigma \in \Sigma_n$ and $t_1, \ldots, t_n$, $n \geqslant 0$ are terms, then

$$t^+ = \sigma(t_1^+, \ldots, t_n^+),$$
$$t^- = \sigma(t_n^-, \ldots, t_1^-).$$

3. If $t = s^{\vee}$ then $t^+ = s^-$ and $t^- = s^+$.

Moreover, if t is a Σ-term, we define
1. $t^R = x$, if $t = x \in X$.
2. $t^R = \sigma(t_n^R, \ldots, t_1^R)$, if $t = \sigma(t_1, \ldots, t_n)$, where $\sigma \in \Sigma_n$ and $t_1, \ldots, t_n$, $n \geqslant 0$ are Σ-terms.

Let $\overline{X} = \{\overline{x} : x \in X\}$ denote a disjoint copy of X whose elements correspond to the elements of X in a bijective manner. The X-generated free algebra in $\mathscr{V}$, denoted $\mathbf{F}_{\mathscr{V}}(X)$, can be considered to be a subalgebra of the $X \cup \overline{X}$-generated free algebra $\mathbf{F}_{\mathscr{V}}(X \cup \overline{X})$. For any $\Sigma^\vee$-term $t = t'(x_1, \ldots, x_n, x_1^\vee, \ldots, x_n^\vee)$ in positive normal form in the variables $x_1, \ldots, x_n$, where t' is a Σ-term, we denote by $|t|$ the element

$$t'_{\mathbf{F}_{\mathscr{V}}(X \cup \overline{X})}(x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n) \in \mathbf{F}_{\mathscr{V}}(X \cup \overline{X}),$$

which is the value of the term function $t'_{\mathbf{F}_{\mathscr{V}}(X \cup \overline{X})}$ induced by t' in the algebra $\mathbf{F}_{\mathscr{V}}(X \cup \overline{X})$ on the given generators. For example, if $\mathscr{V}$ is the variety of all Σ-algebras, and $t = (\sigma(x^\vee))^\vee$, $s = (\sigma(x))^\vee$, then $|t^+| = \sigma(x)$, $|s^+| = \sigma(\overline{x})$, so that $|t^+|$ is in $F_{\mathscr{V}}(X)$ and $|s^+| \notin F_{\mathscr{V}}(X)$.

Suppose that Ax is a set of equations between $\Sigma^\vee$-terms. Given terms t, t', we write $t \to_{Ax} t'$ if t' can be obtained from t by replacing a subterm which is a substitution instance of the term appearing on one side of an equation in Ax by the corresponding substitution instance of the term on the other side of the equation. It is well known that an equation $t = t'$ is a logical consequence of Ax iff $Ax \vdash t = t'$, i.e., when there is a sequence $t_0, \ldots, t_k$ of terms such that $t_0 = t$, $t_k = t'$ and $t_{i-1} \to_{Ax} t_i$ holds for each $i = 1, \ldots, k$.

Below we will call a set E_0 of equations between Σ-terms *closed for reversal* if $t_1^R = t_2^R$ is in E_0 for any equation $t_1 = t_2$ in E_0.

Let *Inv* denote the collection of the involution equations (1), (2).

Lemma 2.1. *Let E_0 denote a set of equations that hold in $\mathscr{V}$ and suppose that a set Ax constitutes a complete equational axiomatization of a variety $\mathscr{W} \subseteq \widehat{\mathscr{V}}$, over the variety $\widehat{\mathscr{V}}$. Assume that the following conditions hold.*
1. *E_0 is closed for reversal.*
2. *If t_1, t_2 are $\Sigma^\vee$-terms such that $t_1 \to_{Ax} t_2$ and $|t_1^+|$ is in $\mathbf{F}_{\mathscr{V}}(X)$, then $E_0 \cup Inv \vdash t_1 = t_2$.*

Then the set $E = E_0 \cup Inv \cup Ax$ is an equational base for $\mathscr{W}$ iff E_0 is an equational base for $\mathscr{V}$. Moreover, $\mathscr{V}$ and $\mathscr{W}$ satisfy the same equations between Σ-terms.

We note the following facts.

Sublemma 2.2. *For any terms t_1 and t_2, $t_1^+ = t_2^+$ iff $Inv \vdash t_1 = t_2$.*

Sublemma 2.3. *Suppose that E_0 is a set of equations between Σ-terms. If E_0 is closed for reversal and $t_1 \to_{E_0} t_2$, for some terms t_1 and t_2, then $t_1^+ \to_{E_0} t_2^+$ and $t_1^- \to_{E_0} t_2^-$.*

Proof. Since $t_1 \to_{E_0} t_2$, there exist an equation $p_1(x_1, \ldots, x_n) = p_2(x_1, \ldots, x_n)$ in E_0 in the variables $x_1, \ldots, x_n$, a term $r(x_1, \ldots, x_m, x_{m+1})$ containing exactly one occurrence of

the variable x_{m+1}, and terms $q_1,\ldots,q_n$ such that

$$t_1 = r(x_1,\ldots,x_m, p_1(q_1,\ldots,q_n)),$$
$$t_2 = r(x_1,\ldots,x_m, p_2(q_1,\ldots,q_n)).$$

We argue by the structure of the term r to prove the claims of the lemma. When $r = x_{m+1}$, we have

$$t_i^+ = p_i(q_1^+,\ldots,q_n^+),$$
$$t_i^- = p_i^R(q_1^-,\ldots,q_n^-), \quad i = 1,2.$$

Thus, $t_1^+ \to_{E_0} t_2^+$ and $t_1^- \to_{E_0} t_2^-$, since $p_1^R = p_2^R$ is in E_0.

There are two subcases in the induction step. Here we only consider the case that $t_1 = s_1^\vee$ and $t_2 = s_2^\vee$, where $s_1^+ \to_{E_0} s_2^+$ and $s_1^- \to_{E_0} s_2^-$. Now $t_1^+ = s_1^-$ and $t_2^+ = s_2^-$, so that $t_1^+ \to_{E_0} t_2^+$ by the induction hypothesis. In the same way, $t_1^- \to_{E_0} t_2^-$. □

Proof of Lemma 2.1. It is obvious that if E_0 is an equational base of $\mathscr{V}$ then E is an equational base of $\mathscr{W}$. Suppose now that the set of equations E is a complete axiomatization of $\mathscr{W}$. We prove that E_0 is an equational base of $\mathscr{V}$.

Suppose that t and t' are Σ-terms such that $t = t'$ holds in $\mathscr{W}$. Then there is sequence of terms $t_0,\ldots,t_k$ such that $t = t_0$, $t' = t_k$ and $t_{i-1} \to_E t_i$ for each $i = 1,\ldots,k$. We claim that $E_0 \vdash t_{i-1}^+ = t_i^+$, for each $i = 1,\ldots,k$. Since $t = t^+$ and $t' = t'^+$, it follows that $E_0 \vdash t = t'$.

We prove $E_0 \vdash t_{i-1}^+ = t_i^+$ by induction on i. There are several subcases in the induction step. If $t_{i-1} \to_{Inv} t_i$, then $t_{i-1}^+ = t_i^+$, by Sublemma 2.2. If $t_{i-1} \to_{E_0} t_i$, then $t_{i-1}^+ \to_{E_0} t_i^+$, by Sublemma 2.3. Suppose now that $t_{i-1} \to_{Ax} t_i$. Since by the induction hypothesis we have $E_0 \vdash t_{j-1}^+ = t_j^+$, for each $j = 1,\ldots,i-1$, it follows that $|t_{i-1}^+| = |t^+|$ is in $\mathbf{F}_{\mathscr{V}}(X)$. Thus, by the second condition of Lemma 2.1, we have $E_0 \cup Inv \vdash t_{i-1} = t_i$, so that $E_0 \vdash t_{i-1}^+ = t_i^+$, by Sublemmas 2.2 and 2.3. □

Corollary 2.4. *Suppose that a finite set of equations Ax constitutes a complete axiomatization of a variety $\mathscr{W} \subseteq \widehat{\mathscr{V}}$, over the variety $\widehat{\mathscr{V}}$. If $\mathscr{V}$ is finitely based, then so is $\mathscr{W}$. Assume that the following conditions also hold.*

- *The set of valid equations of $\mathscr{V}$ is closed for reversal.*
- *There exists a finite set F of equations that hold in $\mathscr{V}$ such that if t_1, t_2 are $\Sigma^\vee$-terms with $t_1 \to_{Ax} t_2$ and $|t_1^+|$ is in $\mathbf{F}_{\mathscr{V}}(X)$, then $F \cup Inv \vdash t_1 = t_2$.*

Then $\mathscr{W}$ and $\mathscr{V}$ satisfy the same equations between Σ-terms, moreover, if $\mathscr{W}$ is finitely based, then so is $\mathscr{V}$.

Proof. Since $\mathscr{W}$ is a subvariety of $\widehat{\mathscr{V}}$, any equation between Σ-terms that holds in $\mathscr{V}$ also holds in $\mathscr{W}$. Moreover, since Inv and Ax are finite, if $\mathscr{V}$ is finitely based then so is $\mathscr{W}$.

Assume that the two additional conditions of Corollary 2.1 also hold. Let E_0 denote a set of valid equations of $\mathscr{V}$ containing the set F that together with the equations Inv and Ax constitutes an equational base E of the variety $\mathscr{W}$. By the first condition, we may as well assume that E_0 is closed for reversal. Since E_0 clearly satisfies the second condition of Lemma 2.1, E_0 is an equational base of $\mathscr{V}$. Moreover, $\mathscr{V}$ and $\mathscr{W}$ satisfy the same equations between Σ-terms, and $\mathscr{V}$ is finitely based if $\mathscr{W}$ is. □

Corollary 2.5. *The varieties $\mathscr{V}$ and $\widehat{\mathscr{V}}$ satisfy the same equations between Σ-terms iff the set of equations that hold in $\mathscr{V}$ is closed for reversal. Moreover, in this case, $\mathscr{V}$ is finitely based iff $\widehat{\mathscr{V}}$ is.*

Proof. It is clear that for any Σ-terms t_1, t_2 we have $Inv \cup \{t_1 = t_2\} \vdash t_1^R = t_2^R$. □

3. Applications

Definition 3.1. A ***-semiring** is a unitary semiring [11] $(S, +, \cdot, 0, 1)$ equipped with a unary operation $^* : S \to S$. A **Conway semiring** [1, 11] is a *-semiring which satisfies the following two equations:

$$(x + y)^* = (x^* y)^* x^*,$$

$$(xy)^* = 1 + x(yx)^* y.$$

Finally, a *-semiring satisfying

$$1^* = 1$$

is called **ω-idempotent**.

Note that any ω-idempotent Conway semiring is idempotent, i.e., satisfies the equation

$$x + x = x.$$

Now we consider Conway's group matrix equations.

Definition 3.2. Let M be an $n \times n$ matrix whose entries are regular expressions, i.e., Σ-terms over the signature Σ with $\Sigma_2 = \{+, \cdot\}$, $\Sigma_1 = \{^*\}$, $\Sigma_0 = \{0, 1\}$ and $\Sigma_n = \emptyset$ for all $n > 2$. We define the matrix M^* by induction on n.

- For $n = 1$ and $M = [r]$ (r is a single regular expression) we define $M^* = [r^*]$.
- Suppose $n = k + 1$, $k \geqslant 1$ and

$$M = \begin{bmatrix} A & B \\ C & D \end{bmatrix},$$

where the dimensions of the blocks A and D are $k \times k$ and 1×1, respectively (while the dimensions of B and C are forced). In that case,

$$M^* = \begin{bmatrix} (A + BD^*C)^* & (A + BD^*C)^*BD^* \\ (D + CA^*B)^*CA^* & (D + CA^*B)^* \end{bmatrix}.$$

Definition 3.3 (*Conway* [4]). Let G be a finite group of order n, say $G = \{g_1, \ldots, g_n\}$. Define the matrix $M_G = [\mu_{ij}]_{n\times n}$ over the given set of variables $X = \{x_1, x_2, \ldots\}$ as follows:

$$\mu_{ij} = x_k \quad \text{if and only if} \quad g_i g_k = g_j.$$

If η_n denotes the $1 \times n$ row matrix with 1 as the first entry and 0 as other entries, and if ε_n denotes the $n \times 1$ column matrix consisting entirely of 1's, then the **group matrix equation associated to** G is the equation

$$\eta_n(M_G)^*\varepsilon_n = (x_1 + \cdots + x_n)^*.$$

We denote this equation by $\Pi(G)$.

Remark 3.4. Suppose that G is a cyclic group of order p. In [4], it is proved that in ω-idempotent Conway semirings, $\Pi(G)$ is equivalent to the equation

$$(1 + x + \cdots + x^{p-1})(x^p)^* = x^*. \tag{3}$$

Recall from the introduction the definition of the varieties $\mathscr{KA}$ and $\mathscr{KA}^\vee$.

Theorem 3.5 (Ésik and Bernátsky [8]). *The variety $\mathscr{KA}^\vee$ is finitely based relatively to $\mathscr{KA}$ and one equational base for $\mathscr{KA}^\vee$ over $\mathscr{KA}$ is given by the involution equations Inv,*

$$(x + y)^\vee = (y^\vee + x^\vee), \tag{4}$$
$$(xy)^\vee = y^\vee x^\vee, \tag{5}$$
$$(x^*)^\vee = (x^\vee)^*, \tag{6}$$
$$0^\vee = 0, \tag{7}$$
$$1^\vee = 1, \tag{8}$$
$$(x^\vee)^\vee = x \tag{9}$$

together with the equation

$$x + xx^\vee x = xx^\vee x. \tag{10}$$

Note that (7) and (8) may be removed as these equations can be derived from the rest of the axioms.

Following [6], we will say that a finite group G *divides* a finite group H if G is a quotient of a subgroup of H.

Theorem 3.6 (Krob [14]). *Let $\mathscr{G}$ denote a subclass of the class of all finite groups. The equations defining ω-idempotent Conway semirings, together with the group matrix equations $\Pi(G)$ for $G \in \mathscr{G}$ form an equational base of the variety $\mathscr{KA}$ iff each finite simple group divides some group in $\mathscr{G}$.*

The above result was formulated in a weaker form in [14]. The present formulation is from [2]. The theorem is deduced from a more general result in [7]. The following corollary was proved in [4, 16].

Corollary 3.7. *The variety $\mathscr{KA}$ is not finitely based.*

For any set A, let A^* denote the free monoid of all finite words over A including the empty word. It is known [5] that $\mathscr{KA}$ is the same as the variety $\mathscr{L}$ generated by the *-semirings

$$\mathbf{Lang}_A = (\mathscr{P}(A^*), +, \cdot, ^*, 0, 1),$$

where $+$ is set union, $\cdot$ is complex concatenation, * is the Kleene star operation and where the constants 0 and 1 are, respectively, the empty set and the set containing only the empty word. It is known that the A-generated free algebra in this variety can be described as the substructure $\mathbf{Reg}_A$ of $\mathbf{Lang}_A$ determined by the regular subsets of A^*. Thus, if t is a $^\vee$-regular expression (i.e., $\Sigma^\vee$-term) in positive normal form, then $|t|$ is just the regular language in $(X \cup \overline{X})^*$ denoted by t.
We now prove:

Theorem 3.8. *The variety $\mathscr{KA}^\vee$ is not finitely based.*

Proof. It is clear that if an equation $t_1 = t_2$ holds in $\mathscr{KA}$, where t_1, t_2 are regular expressions, then so does the equation $t_1^R = t_2^R$. Thus, by Corollary 2.4, all we need to prove is that there is a finite set F of valid equations of the variety $\mathscr{KA}$ such that the following condition holds for any $^\vee$-regular expressions t_1 and t_2: If $|t_1^+| \in \mathbf{Reg}_X$ and $t_1 \to_{E_0} t_2$, where E_0 consists only of (10), then $F \cup Inv \vdash t_1 = t_2$.

By assumption, t_2 can be obtained from t_1 by replacing a subterm of the form $pp^\vee p + p$ with the term $pp^\vee p$, or the other way around. Since the language $|t_1^+|$ contains no word having an occurrence of any letter in $\overline{X}$, this is possible only if $pp^\vee p + p$, or $pp^\vee p$, occurs inside a subterm q of t_1 such that the language denoted by q is the empty set, or if p denotes the set consisting only of the empty word. In either case, it follows easily that $F \cup Inv \vdash t_1 = t_2$, where F consists of the equational axioms of ω-idempotent Conway-semirings. □

Remark 3.9. Using Lemma 2.1 together with Theorems 3.5, 3.6 and the fact that in conjunction with the Conway identities, each group matrix equation implies its reversal,

we can prove the following version of Theorem 3.6. Let $\mathscr{G}$ denote a subclass of the finite groups. Then the set consisting of the idempotent Conway semiring equations, the group matrix equations associated with the groups in $\mathscr{G}$, the involution equations and Eq. (10) is an equational base of $\mathscr{KA}$ iff every finite simple group divides some group in $\mathscr{G}$. However, we will prove this result by different methods.

We briefly mention some other applications of Corollary 2.4, and in particular of Corollary 2.5. First, since $\mathscr{KA}^{\vee}$ is not finitely based, it follows immediately that the variety $\mathscr{L}^{\vee} = \widehat{\mathscr{L}}$ is also not finitely based. However, this result is also a direct consequence of Corollary 2.5 and Corollary 3.7. The variety $\mathscr{L}^{\vee}$ is of interest in automata and language theory, since it is determined by the above language structures $\mathbf{Lang}_A$ equipped with the operation $^{\vee}$ of *reversal* [3].

The enrichment of language structures $\mathbf{Lang}_A$ with both the operations of *shuffle* and reversal has been considered in [10]. Denoting the shuffle operation by $\otimes$, for each set A, let

$$\mathbf{SL}_A = (\mathscr{P}(A^*), +, \cdot, \otimes, 0, 1),$$
$$\mathbf{SL}_A^{\vee} = (\mathscr{P}(A^*), +, \cdot, \otimes, ^{\vee}, 0, 1).$$

Moreover, let $\mathscr{SL}$ and $\mathscr{SL}^{\vee}$ denote the variety generated by the structures $\mathbf{SL}_A$ and $\mathbf{SL}_A^{\vee}$, respectively. Now $\mathscr{SL}$ is not finitely based [9] and $\mathscr{SL}^{\vee}$ is finitely axiomatized over $\mathscr{SL}$ by the involution identities [10]. Thus, $\mathscr{SL}^{\vee}$ is also not finitely based. Similar facts hold if one also considers the *-operation.

4. Conway's models

Definition 4.1. Let G be a finite group. We define **Conway's model over** G to be the algebra

$$\mathbf{C}(G) = (\mathscr{P}(G^{\infty}), +, \cdot, ^*, 0, 1),$$

where G^{∞} is the 0-group obtained by adjoining a zero element ∞ to G (that is, $\infty \cdot a = a \cdot \infty = \infty$ for all $a \in G$ and $\infty^2 = \infty$). The sum of $A, B \subseteq G^{\infty}$ is their union, and the product AB is the complex product defined by

$$AB = \{ab\colon a \in A,\ b \in B\}.$$

The constants 0 and 1 are the empty set $\emptyset$ and the set $\{e\}$ containing only the identity element of G, respectively. Finally, the star operation is defined in the following way ($\langle A \rangle$ is the submonoid of G^{∞} generated by A):

$$A^* = \begin{cases} \langle A \rangle & \text{if } \langle A \rangle \neq G, \\ G^{\infty} & \text{otherwise.} \end{cases}$$

Lemma 4.2. *For each finite group G, $\mathbf{C}(G)$ is an ω-idempotent *-semiring.*

Proof. The semiring axioms are obviously satisfied, while the equation $1^* = 1$ holds because G contains a trivial subgroup. □

The key result, which brings connection between group matrix equations, Conway's models, and the structural properties of finite groups, is the following.

Proposition 4.3 (Krob [14]). *Assume G is a finite simple group. Then Conway's model $\mathbf{C}(G)$ is an ω-idempotent Conway semiring. Moreover, if K is any finite group, then $\Pi(K)$ holds in $\mathbf{C}(G)$ iff G does not divide K.*

One direction of the above equivalence is, in fact, an extension of Theorem 6, p. 116 of Conway's book [4], while the other was most probably known to him (at least for the case that G is a nonsolvable group), cf. Theorems 7–9, pp. 117–118 in [4].

We proceed by introducing a new operation on $\mathscr{P}(G^\infty)$. Its task will be to "cover" the conversion operation in Kleene algebras, in other words, to incorporate the equations given in Theorem 3.5 into Conway's models.

When a is a group element, let a^{-1} denote its inverse. Moreover, let $\infty^{-1} = \infty$.

Definition 4.4. Suppose that G is a finite group. For $A \subseteq G^\infty$, we define

$$A^\vee = \{a^{-1} : a \in A\}.$$

We call the algebra

$$\mathbf{C}^\vee(G) = (\mathscr{P}(G^\infty), +, \cdot, ^*, ^\vee, 0, 1)$$

the **involution Conway's model over** G, provided that its $^\vee$-free reduct is Conway's model $\mathbf{C}(G)$ and the operation $^\vee$ is defined as above.

Lemma 4.5. *Let G be a group. Then $\mathbf{C}^\vee(G)$ is an involution *-semiring satisfying Eq.* (10).

Proof. The first part of the proof follows from Lemma 4.2. Eq. (4) is obviously satisfied, as well as Eq. (9), because $(a^{-1})^{-1} = a$ for all $a \in G^\infty$. Eq. (5) also follows easily, because $(ab)^{-1} = b^{-1}a^{-1}$ holds not only for all $a, b \in G$, but also in the case that a or b is ∞. Further, note that for $A \subseteq G^\infty$ containing an element $a \neq \infty$ we have

$$A = A\{a^{-1}\}\{a\} \subseteq AA^\vee A,$$

while for $A = \emptyset$ or $A = \{\infty\}$ the inclusion $A \subseteq AA^\vee A$ follows immediately. Hence, Eq. (10) is satisfied by $\mathbf{C}^\vee(G)$.

Thus it remains to verify Eq. (6). First, note that for each $A \subseteq G^\infty$, A^* is either a subgroup of G or the union of a subgroup of G and $\{\infty\}$. Therefore, $(A^*)^\vee = A^*$.

On the other hand, each set $A \subseteq G$ generates the same subgroup of G as $A^\vee$. Also, A contains ∞ if and only if $A^\vee$ does. This observation implies $(A^\vee)^* = A^*$ and so Eq. (6) is confirmed to hold in the considered algebra. □

The ω-idempotent Conway involution semiring equations are the defining equations of ω-idempotent Conway semirings together with Eqs. (4)–(6) and (9).

Theorem 4.6. *Suppose that $\mathscr{G}$ is a subclass of the finite groups. The set $E_{\mathscr{G}}$ consisting of the ω-idempotent Conway involution semiring equations, the group matrix equations associated with the groups in $\mathscr{G}$, and Eq.* (10) *is an equational base of $\mathscr{KA}^\vee$ iff every finite simple group divides a group in $\mathscr{G}$.*

Proof. If every finite simple group divides some group in $\mathscr{G}$, then $E_{\mathscr{G}}$ is an equational base of $\mathscr{KA}^\vee$, by Theorems 3.5 and 3.6. Suppose now that $E_{\mathscr{G}}$ is an equational base of $\mathscr{KA}^\vee$, for some subclass $\mathscr{G}$ of the finite groups. Suppose that G is a finite simple group and consider the involution Conway's model $\mathbf{C}^\vee(G)$. If G does not divide any group in $\mathscr{G}$, then, by Proposition 4.3 and Lemma 4.5, $\mathbf{C}^\vee(G)$ satisfies all identities in $E_{\mathscr{G}}$. On the other hand, $\Pi(G)$ fails in $\mathbf{C}^\vee(G)$. This contradicts the fact that $\Pi(G)$ holds in $\mathscr{KA}^\vee$. □

Let us define the following relation $\approx$ on $\mathscr{P}(G^\infty)$: For $A, B \subseteq G^\infty$, $A \approx B$ iff $A = B$ or $\infty \in A \cap B$. This relation is easily seen to be a congruence relation of $\mathbf{C}^\vee(G)$. We could have used the models $\mathbf{C}^\vee(G)/\approx$ in place of the models $\mathbf{C}(G)$ in the proof of Theorem 4.6. When G is the cyclic group of order p, let us denote $\mathbf{C}^\vee(G)/\approx$ by $A_p^\vee$. The $^\vee$-free reduct of this algebra is just the model A_p defined on p. 106 in [4]. Assuming that $\mathscr{KA}$ is finitely based, it has an equational base, which, in addition to the involution equations and (10), consists of a finite set E of equations that hold in $\mathscr{KA}$. It is shown in [4] that there is a prime number p such that all equations in E hold in A_p. Thus, since the involution equations and (10) hold in $A_p^\vee$ but Eq. (3) fails, we have

Corollary 4.7. *For each finite set of equations E that hold in $\mathscr{KA}^\vee$ there is an equation $t = t'$* **in one variable** *which also holds in $\mathscr{KA}^\vee$ but $E \not\vdash t = t'$.*

Open problems. Using the above methods, it was shown in [4] that any equational base of the variety $\mathscr{KA}$ contains infinitely many equations in at least two variables. We conjecture that the same holds for $\mathscr{KA}^\vee$.

As shown in [15], it is possible to enlarge the set of operations on relations such that there exists a finite set of valid identities that proves all Kleene algebra identities of $\mathscr{KA}$. The same is true if one also adds conversion. Nevertheless, the following problem seems to be open. Can one add a few natural operations to the collection of operations on relations we have been considering such that the variety generated by the resulting structures is finitely based?

References

[1] S.L. Bloom, Z. Ésik, Equational axioms for regular sets, Math. Struct. Comput. Sci. 3 (1993) 1–24.
[2] S.L. Bloom, Z. Ésik, The equational logic of fixed points, Theoret. Comput. Sci. 179 (1997) 1–60.
[3] S.L. Bloom, Z. Ésik, Gh. Stefanescu, Notes on equational theories of relations, Algebra Universalis 33 (1995) 98–128.
[4] J. Conway, Regular Algebra and Finite Machines, Chapman & Hall, London, 1971.
[5] S. Crvenković, R.Sz. Madarász, On Kleene algebras, Theoret. Comput. Sci. 108 (1993) 17–24.
[6] S. Eilenberg, Automata, Languages, and Machines, vol. 2, Academic Press, New York, 1976.
[7] Z. Ésik, Group axioms for iteration, Inform. and Comput. 148 (1998) 131–180.
[8] Z. Ésik, L. Bernátsky, Equational properties of Kleene algebras of relations with conversion, Theoret. Comput. Sci. 137 (1995) 237–251.
[9] Z. Ésik, M. Bertol, Nonfinite axiomatizability of the equational theory of shuffle, Acta Inform. to appear. Extended abstract in: proc. ICALP'95, Lecture Notes in Computer Science, vol. 944, Springer, Berlin, 1995, pp. 27–38.
[10] Z. Ésik, M. Katsura, M. Ito, The equational theory of reversal, Proc. Int. Workshop on Formal Languages and Computer Systems, Kyoto '97, World Scientific, Singapore, to appear.
[11] J.S. Golan, The Theory of Semirings with Applications in Mathematics and Theoretical Computer Science, Longman Scientific and Technical, New York, 1993.
[12] G. Grätzer, Universal Algebra, Springer, Berlin, 1979.
[13] B. Jónsson, The theory of binary relations, in: Algebraic Logic, Colloq. Math. Soc. János Bolyai, vol. 54, North-Holland, Amsterdam, 1988, pp. 245–292.
[14] D. Krob, Complete systems of B-rational identities, Theoret. Comput. Sci. 89 (1991) 207–343.
[15] V.R. Pratt, Action logic and pure induction, in: Logics in AI: European Workshop JELIA '90, Lecture Notes in Computer Science, vol. 478, Springer, Berlin, 1991, 97–120.
[16] V.N. Redko, On defining relations for the algebra of regular events, Ukrainian Math. J. 16 (1964) 120–126 (in Russian).
[17] A. Salomaa, Two complete axiom systems for the algebra of regular events, J. ACM 13 (1966) 158–169.